08/777246

- 1 -

TITLE

Method and Apparatus for Input of Coded Image Data

5

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to an image input apparatus and to a method for preventing forgery of image data.

10

Related Background Art

Image input systems which convert an image to digital image data should be capable of providing high definition image at low cost. Accordingly, there has

15 been developed image input apparatus which is capable of producing a high definition image with highly efficient coding.

Prior input apparatus which processed analog image

20 signals were not subject to easy forgery. However, recently developed digital image input systems which process images in digital form have been subject to easy forgery. As a result, the credibility of the output image data is weakened.

25

SUMMARY OF THE INVENTION

This invention is directed to overcoming the above described problem. It is an object of the invention to provide an image input apparatus and method which can

30 ensure the integrity of digital image data. This

method and apparatus makes use of digital signature technology.

According to a publication of Eizi Okamoto of Kyouritu
5   Syuppan, Inc., a digital signature assures that the person who purports to generate a message or information is the true author of the message. This digital signature may be used by the recipient of the message as assurance that the information contained
10   therein is true.

According to the invention, an image input apparatus generates a particular digital signature in relation to image data; and outputs this digital signature together
15   with the digital image data.

In an image receiving system, an entity which receives the digital image data and the digital signature will be able to ascertain the authenticity of the image data
20   by checking the relation between the image data and the digital signature. And, if the relation between the image data and the digital signature is inappropriate, the receiving entity will judge that the image data has been falsified or altered. Thus, the image input
25   apparatus and the image receiving system guarantee the authenticity of the image data and its credibility as evidence.

BRIEF DESCRIPTION OF THE DRAWINGS
30   Fig. 1 is a block diagram showing an embodiment of the invention;
Fig. 2 is a block diagram for a digital camera which serves as an image input apparatus;
Fig. 3 is a block diagram showing an embodiment of a n
35   image input system;
Fig. 4 is a data format outputted by the image input system;

Fig. 5 is a block diagram of an image input system
which outputs a digital signature; and
Fig. 6 is a data format outputted by the image input
system.

5

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS
The First Embodiment
In the first embodiment of the invention, a public key
cryptography is applied to an image input apparatus as
10   an algorithm of a digital signature. The apparatus
uses a secret key corresponding to the public key as
its own secret information.

It should be understood that this embodiment is only
15   one example. Another embodiment may be realized by
using another algorithm instead of the public key
cryptography, provided that the other algorithm is able
to verify original information which is being based
upon the original information and the secret
20   information.

First, a public key cryptography will be described.
Then an image unit will be described as well as a
detailed process for a digital signature. Finally, the
25   process for verifying the digital signature will be
described.

(Public-key Encryption System)
Public-key cryptography is one type of cryptography.
30   Public-key cryptography uses two different keys,
namely, an encryption key and a decryption key. In
public key cryptography, the encryption key is
published, but the decryption key is not published.

35   Public-key cryptography provides a certification
function which assures to the receiver that transformed
information has not been changed and that the sender is

not a pretender. Generally, public-key cryptography
has been considered as one of the most effective
methods for protecting data.

5   The operation for encrypting an original message (M) by
using a public key (PK) is: E(PK, M). The operation
for decrypting the encrypted message (M) by using a
secret key (SK) must satisfy the following two
conditions:

10   (1) The operation for encryption E(PK, M) must be
easily carried out using the public key PK and the
operation for decryption D(SK, M) must be easily
carried out using the secret key SK by a person who
knows the secret key SK; and

15   (2) Even if the user has both the public key PK
and the process or operation for encrypting E(PK, M),
it must be nearly impossible to obtain the original
message M without the secret key SK in view of the
extremely large number of operations that would have to
20 be carried out for determining the original message M.

A secret communication will be able to be realized by
satisfying the above conditions (1) and (2) and the
following condition (3):

25   (3) The operation for encrypting all original
message M with the public key PK must be possible; and
the operation for decryption D(SK, E(PK, M)) must
produce a recognizable message (M);

$$i.e.\ D(SK,\ E(PK,\ M)) = M.$$

30 This means that anyone will be able to encrypt the
message (M) by using the public key PK; but only a
person who knows the secret key SK will be able to
decrypt the encrypted message.

35 On the other hand, certification will be realized by
satisfying conditions (1) and (2) and the following
condition (4):

(4)   The operation for decrypting a message (M) with the secret key SK is possible; and the operation for encrypting $E(PK, D(SK, M)) = M$ must be possible.

5   This means that only a person who knows the secret key SK will be able to decrypt the message (M) by using the secret key SK. So, if someone who has a different secret key SK', and pretends to be a person who knows the secret key SK, tries to decrypt the message (M) by
10 using that secret key SK', he will not be able to obtain the message (M);
    i.e. $E(PK, D(SK', M)) \neq M$.
The receiver will therefore find out the forgery carried out by some third party.
15

On the other hand, if $D(SK, M)$ is altered by someone, for example, to $D(KS, M)'$, he will not be able to obtain the message (M);
    i.e. $E(PK, D(SK, M)') \neq M$.
20 Therefore, in this case also, the receiver will find out the modification carried out by the illicit act of a third party.

The result of the operation for decrypting $D(SK, M)$ is
25 referred to as: "A Digital Signature for Text M".
    The typical public key cryptography is as follows.
    Cryptography which can realize both secret communications and authenticated communications is known as:
30   "RSA cryptography" - (R. L. Rivest, A. Shamir and L. Adleman: "A Method of Obtaining Digital Signatures and Public-key Cryptosystems", Comm. of ACM 1987);
    "R cryptography" - (M. Rabin: "Digitalized Signatures and Public-key Cryptosystems", MIT/LCSTR-
35 212, Technical Report MIT. 19797);
    "W cryptography" - (H. C. Williams: "A Modification of the RSA Public-key Encryption

Procedure", IEEE Trans. Inf. Theory, IT-26, 6, 1980);
and

"MI cryptography" - (T. Matsumoto and H. Imai: "A
Class of Asymmetric Cryptosystems Based on Polynomials
5 Over Finite Rings", IEEE International Symp. on
Information Theory, 1983), etc.

Cryptography which can realize secret but
authenticated communications is known as:

"MH cryptography" - (R. C. Merkle and M. E.
10 Hellman: "Hiding Information and Signatures in Trapdoor
Knapsacks", IEEE Trans. Inf. Theory, IT-24, 5, 1987;

"GS cryptography" - (A. Shamir and R. E. Zippel:
"On the Security of the Merkle-Hellman Cryptographic
Scheme", IEEE Transs. Inf. Theory, IT-26, 3, 1980);

15 "CR cryptography" - (B. Chor and R. L. Rivest: "A
Knapsack Type Public-key Cryptosystem Based on
Arithmetic Infinite Field", Proc. Crypto84);

"M cryptography" - (R. J. McElice: "A Public-key
Cryptosystem Based on Algebraic Coding Theory", DSN
20 Progress Rpt., Jet Propulsion Lab., 1978);

"E cryptography" - (T. E. El Gamel: "A Public-key
cryptocsystem and Signature Scheme Based on Discrete
Logarithms", Proc. Crypto84, 1984));

"T cryptography" - (Sigeo Tsuzii: "A Public-key
25 System Based on Matrix Analysis" [*Japanese*], IT85-12,
1985, etc.

Cryptography which is able to realize
authenticated communications but secret communications
is known as:

30 "S cryptography" - (A. Shamir: "A FastSignature
Scheme", Report MIT/LCS/TM-107, MIT Laboratory for
Computer Science, Cambridge, Mass., 1978);

"L cryptography" - (K. Liberherr: "Uniform
Complexity and Digital Signature", Lecture Note in
35 Computer Science 115 Automata, Language and
Programming, Eighth Colloquium Acre, Israel, 1981):

"GMY cryptography" - (S. Goldwasser, S. Micali and A. Yano: "Strong Signature Schemes", ACM Symp. on Theory of Computing, 1983);

"GMR cryptography" - (S. Goldwasser, S. Micali and
5   R.L. Rivest: "A Paradoxical Solution to the Signature Problem", ACM Symp. on Foundation of Computer Science, 1984);

"OSS cryptography" - (H. Ong, C. P. Schnorr and A. Shamir: "An Efficient Signature Scheme Based on
10   Quadratic Equations", ACM Symp. on Theory of Computing 1984);

"OS cryptography" - (T. Okamoto and A. Shiraisi: "A Fast Signature Scheme Based on Quadratic Inequalities", IEEESymp. on Theory of Computing, 1984),
15   etc.

(Construction of the Image Input Device)

An embodiment of the invention to which digital
20   signature based on the public-key cryptography is applied will be described hereinbelow with reference to Fig. 1.   In Fig. 1. an image input device, such as a digital camera, is shown by functional blocks.   A line which connects the blocks represents a control and data
25   bus.

The image input device includes an image pick up part 1 which converts an optical image into an electrical signal.   The image pick-up part 1 includes a signal
30   processor, an analog-to-digital converter, an image processor and a coder.   The electrical signal is processed in the processor, converter and coder and is output as a digital signal.

35   The image input device also includes: a controller 2 (CPU) for controlling the image input device by performing predetermined operations based on control

software stored in a memory; a memory 3 for storing the control software; a work memory 4 for use during operation of the apparatus; an operation switch 5 for inputting commands and designating an area of an image

5 for the digital signature of a user; a mechanical portion 6 for controlling mechanical operations of the image input device based on commands from the controller 2; and a main memory 7 for storing the processed image output. The mechanical portion 6, for

10 example, includes motor and an optical system, composed of a lens and a shutter. In addition, the image input device also includes: an external interface 8 for connecting the input device with other external devices, for example a personal computer, a memory

15 device, etc., for transferring image data or control software to such external devices; and a generator 9 for generating a digital signature for the inputted image data based upon a predetermined algorithm.

20 The above described image input device operates to obtain image data in the following manner. A user initiates an input command by operating the operation switch 5. This causes the controller 2 to respond to the command and control software to control the image

25 portion 1 and the mechanical portion 6. Thereafter, image data is supplied to the generator 9; and the generator 9 produces a digital signature which corresponds to an area of the image represented by the image data. The image data and digital signature are

30 recorded and/or sent to the external device via the interface 8, according to a command.

Alternatively, the image data is first stored in the memory 3; and thereafter only a part of the image data,

35 which corresponds to one area of the image recorded in the memory, is read out and is fed to the generator 9.

The generator 9 generates the digital signature based on this image data for this area.

One embodiment, which is used as a camera for producing
5   digital images and can produce a digital signature based on a public-key cryptography, has a secret key SKcam. In this embodiment, the secret key SKcam, and an algorithm for generating the digital signature Dcam, are stored in the generator 9. In addition, a public
10   key PKcam and an algorithm for verifying an Ecam are known by the entity who wishes to check the integrity of the information. The procedure for generating the digital signature is described below.

15   (Digital Signature Generation)

Image data (I) is generated by the image pick-up part 1 and is fed to the generator 9. The generator 9 carries out an operation by using the secret key (SKcam) and an
20   algorithm for generating a digital signature; and outputs the digital signature (Dcam (SKcam, I)). The image data (I) and the digital signature (Dcam (SKcam, I)) are recorded in the memory 7 and/or are output to an external device via the interface 8.
25

The detailed procedure for verifying that the image data (I) and the digital signature corresponding to the image data (I) are actually generated by the same image input device is described below. In this embodiment,
30   an image input system consists of the image input device and verifying means.

(Digital Signature Verification)

35   The image data (I') and the digital signature (D'cam (SKcam, I)) are verified by carrying out the following

operation using a public key (PKcam) and the algorithm
for verifying the digital data (Ecam);
    i.e. I' = Ecam (PKcam, D'cam (SKcam, I)).
If the above equation produces a recognizable image,
5 the image data (I') is the image data (I) which was
input from the image pick-up part. On the other hand,
if the above equation does not produce a recognizable
image, the image data (I') is not the image data (I).
Accordingly, the verifier can determine whether the
10 image data (I') was modified or forged.

According to this embodiment, the digital signature is
generated based on the same area of the image
designated by the user. Therefore, the time for
15 generating the digital signature can be shortened; and
the load requirements of the system can be reduced.

(The Second Embodiment)

20 The second embodiment, which uses a public key
cryptography as an algorithm for digital signature and
a secret key which is stored in the external device, is
described herein in reference to Fig. 1. In this
embodiment, the external device which stores the secret
25 keys of registered users (SKman) (corresponding to each
registered user's public key (PKman)) and an algorithm
for generating a digital signature (Dman)
(corresponding to an algorithm for verifying the
digital signature), is a portable device. This device
30 is a data processing device; and it is connected to the
image input device via the interface 8. On the other
hand, the public key (PKman), and the algorithm for
verifying the digital signature, are known by the
entity who also wishes to check the integrity of the
35 input image data.

The basic operation for inputting image data is
described as follows. When inputting (for example,
photographing), information, the external device is
connected to the input device via the interface 8. The
5   user inputs a command for photographing by operating
the switch 5 and a command for generating the digital
signature by inputting his own user's number (which is
similar to an identification number). The controller
then ascertains the user's number and controls the
10   image pick-up part 1 and the mechanical part 6 based on
the control software stored in the memory 3. The image
data is then fed to the generator 9. If the user's
number is correct, i.e. if it coincides with one of the
registered numbers, the controller 2 communicates with
15   the external device via the interface 8 and gets the
secret key (SKman) of the user and the algorithm for
generating the user's digital signature. The
controller 2 then carries out an operation using the
user's secret key (SKman) and the algorithm to generate
20   the user's digital signature. The digital signature
and the image data are recorded and/or output to the
external device according to command. In the above
described embodiment, the detailed procedure for
generating the digital signature is as follows:
25

(Digital Signature Generation)

The controller 2 ascertains the user's number and
downloads the secret key (SKman) and the algorithm for
30   generating the digital signature from the external
device, via the interface 8; and enters them into the
memory 4. The image data generated by the image pick-
up part 1 is fed to the generator 9. The generator 9
carries out an operation by using the secret key
35   (SKman) and the algorithm for generating a digital
signature; and it outputs the digital signature (Dman
(SKman, I)). The image data (I) and the digital

signature (Dman (SKman, I)) are recorded in the memory
7 and/or are output to the external device via the
interface 8.

5 The detailed procedure for verifying that the image
data (I) and the corresponding digital signature have
actually been generated by the above input image device
when the external device is connected with the input
image device, is as follows:

10

(Digital Signature Verification)

Image data (I)' to be examined and the digital
signature (D'man (SKman, I)) to be examined are

15 verified by carrying out an operation which uses a
public key (PKman) for verifying the digital data
(Ecam).

i.e.   I' = Eman (PKman Dman (SKman, I)).

If the equation produces a recognizable image, the

20 image data (I') is the image data that was input by the
image input device. On the other hand, if the equation
does not produce a recognizable image, the image data
I' is known to be not the true image data (I); and that
the examined image data (I') has been modified by a

25 different person at a different place. Consequently,
the user can determine that the examined image data
(I') is modified or forged data. Accordingly, an image
input system which guarantees that the image has been
input by the external device is realized in this

30 embodiment.

In this embodiment, the users' numbers are changed or
another user's number is additionally registered by a
person who is authorized to change or add to the user

35 numbers. Therefore, impersonation can be absolutely
prevented.

(Third Embodiment)

The third embodiment, which uses a public key
cryptography as the algorithm for a digital signature,
5   and in which a secret key is stored in an external
device which can operate on the data, is described
hereinbelow, also with reference to Fig. 1.

(Digital Signature Generation)
10

The controller 2 transfers the image data, which was
generated by the image pick-up part 1, to the external
device via the interface 8. The generator 9 in the
external device caries out an operation by using the
15   user's secret key (SKman) and the image data based on
the algorithm for generating a digital signature. The
external device then outputs the digital signature
(Dman (SKman, I)) and the image data and transfers them
to the image input device via the interface 8. In the
20   image input device, the transferred image data (I) and
the digital signature (Dman (SKman, I)) are recorded in
the memory 7 and/or outputted to the external device
via the interface 8.

25

The detailed procedure for verifying that the image
data (I) and the digital signature corresponding to the
image data (I) have actually been generated by the
above image input device when the external device is
30   connected with the image input device, will now be
described.

(Digital Signature Verification)

35   Verification in the third embodiment is the same as in
the second embodiment.

(The Fourth Embodiment)

The fourth embodiment, which uses a public key cryptography as an algorithm for digital signature. In this embodiment, respective secret keys are stored in both the external device and in the image input device, will now be·described, again with reference to Fig. 1.

(Digital Signal Generation)

The controller 2 downloads the secret key (SKman) and the algorithm for generating the digital signature (Dman) into the memory 4 and into the controller 2, from the external device via the interface 8. The image data (I) which was generated by the image pick-up part 1 is fed into the generator 9 in the image input device. The generator 9 caries out an operation by using the secret key SKman and the digital signature (Dman (SKman, I)) based on the algorithm for generating the digital signature (Dman); and outputs the digital signature of the camera Dcam(SKcam, Dman(SKman, I)). The image data (I) and the digital signature of the camera Dcam(SKcam, Dman(SKman, I)) are recorded in the memory 7 and/or outputted to an external device via the interface 8.

The detailed procedure for verifying that the image data (I) and the digital signature corresponding to the image data (I) have actually been generated by the particular external device when that external device is connected with the image input device, will now be described.

(Digital Signature Verification)

The received image data (I') and the received digital signature D'cam(SKcam, Dman(SKman, I)) are verified by

carrying out the following operation using the public
key PKcam and the algorithm for verifying the digital
data Ecam, the algorithm for verifying the digital data
Eman and the public key PKman; i.e.

5   I' = Eman(PKman, Ecam(PKcam, D'cam(SKcam,
Dman(SKman,I))).

If the operation produces a recognizable signature,
this shows that the examined image data (I') is the
10 true image data (I) which was input from the image
input device. On the other hand, if the operation is
not good, the examined image data (I') is seen to be
not the true image data (I); and that it has been
modified by another person or at another location. The
15 user can thus determine that the examined image data
(I)' has been modified or forged. Therefore, this
embodiment provides an image input system which
guarantees that the correct image is input from the
external device. It will be seen that the reverse
20 order of generating the digital signature, by the image
input device and the external device and verifying the
digital signature, will provide the same result. Also,
the algorithm for generating the digital signature in
the external device may be stored in the image input
25 device.

(The Fifth Embodiment)

In this embodiment, the image input device generates
30 the digital signature by using compressed image data.
The compressed data transform is represented herein as
"C" ; and the entity who wishes to verify that the
image data is correct knows the compressed data
transform "C". The image input device in this
35 embodiment is the same as in the above described
embodiments.

(Digital Signature Generation)

The controller 2 carries out its operation using
compressed image data for generating the digital
5   signature rather than the image data which is input by
the image input part 1. The other procedures involved
in the generation of the digital image signature are
the same as in the above embodiments. For example, the
image data and the digital signature D'cam(SKcam, c(I))
10 is verified by using the algorithm for verifying the
digital signature Ecam and the pubic key PKcam; i.e.
the verification conforms to the following equation:

$$C(I') \stackrel{?}{=} Ecam(PKcam, D'cam(SKcam, C(I)))$$

15

If the above equation holds, the examined image data
(I') is seen to be the image data that had been input
by the image input device. On the other hand, if the
equation does not hold, the examined image data (I') is
20 seen to be different from the original image data (I).
In this manner the verifier can confirm that the image
data (I') is modified or forged information.

(The Sixth Embodiment)

25

In this embodiment, the image input device is a digital
camera; and a public key algorithm is used as the
cryptography for generating and verifying the digital
signature. In addition, both the digital camera and
30 the external device have their own secret key for use
with the public key encrypted information. This
embodiment is described hereinbelow with reference to
Fig. 2.

35 (The Construction of the Digital Camera)

In Fig. 2, each block represents a functional portion
of the digital camera; and each line which connects the
blocks represents a control or data bus. The digital
camera has an image input portion 10 (IMG) which

5   converts an optical image into an electrical signal, a
signal processor 11 (PRC) which includes an analog-to-
digital converter, and an image processor, a coder and
a converter which processes the electrical signal and
outputs a digital signal. The digital camera also

10 includes: a controller 12 (CPU) for performing
predetermined operations based on a control program; a
memory 13 (ROM) for storing the control program; a work
memory (i.e. a DRAM) 14 which is used as a work area;
an operation switch 15 (OP-SW) for inputting commands

15 by the user; a microphone 16 (MIC) for the input of
audio information; a main memory 17 (STRG) for storing
the output (i.e. image and audio data and/or
information regarding a situation or condition for
photographing) of the image input portion 10 and/or the

20 microphone 16, etc.

In addition, the digital camera has: an external
interface 18 (I/F) for connecting the camera with an
external device (for example, a personal computer, a

25 memory device, etc.) and for communicating the image
data and/or control software with the other external
device; a generator 19 (CODEC) for generating a digital
signature for the image data and/or audio data based on
a predetermined algorithm; an interface 20 for a PCMCIA

30 card based on PCMCIA standards. Also, the digital
camera has a liquid crystal display (LCD) display 21
and a light emitting diode (LED) type lamp 22.

The basic operation for generating image data with this

35 digital camera will now be described. The external
device is connected with the interface 18; and the user
inputs commands by operation of the switch 15. The

controller 12 communicates with the external device,
and the controller 12 controls the image input portion
10 and processes a compressed image data, etc. by using
the secret key, the algorithm for generating the
5 digital signature stored in the external device and the
secret key, and the algorithm for generating the
digital signature stored in the digital camera.

The image data and the digital signature are recorded
10 and/or sent to the external device via the interface 18
or the PCMCIA interface 20, based on command.
Alternatively, the image data is first stored in the
memory 3, and thereafter the data is read out from the
memory 3 and fed into the generator 9. The generator 9
15 generates the digital signature based on this data.

An embodiment comprising a camera as above described,
may be used for the generation of a digital signature
based on public-key cryptography. The camera described
20 in this embodiment has a secret key. The secret key of
the camera is expressed as SKcam. The algorithm of the
camera for generating the digital signature is
expressed as Dcam; the algorithm for verifying the
digital signature is expressed as Ecam; the public key
25 is expressed as PKcam; and the algorithm for data
compression is expressed as H. Also in this
embodiment, the secret key stored in the external
device is expressed as SKman; the algorithm for
generating the digital signature is expressed as Dman;
30 the algorithm for verifying the digital signal is
expressed as Eman; and the public key is expressed as
PKman.
Further, in this embodiment, the algorithm for
verifying the digital signature Ecam and the public key
35 PKcam of the digital camera, the algorithm for
verifying the digital signature Eman and the public key
PKman of the external device and an algorithm for

compressing the data H, are known by the entity who
wishes to verify to correctness of the data.

The procedure for generating the digital signature will
5 be described hereinbelow.

(Digital Signature Generation)

The image data (I) generated by the image input part 11
10 is fed to the generator 19. The generator 19 caries
out an operation by using the secret key SKcam and the
algorithm for generating the digital signature Dcam;
and outputs the digital signature Dcam(SKcam, H(I)) to
the external device via the interface 18. The external
15 device caries out an operation by using the secret key
SKman and the algorithm for generating the digital
signature Dman and the digital signature Dcam(SKcam,
h(I)) and returns the digital signature Dman(SKman,
Dcam(SKcam, h(I))) to the digital camera via the
20 interface 18. The image data (I) and the digital
signature Dman(SKman, Dcam(SKcam, h(I)) are recorded in
the memory 17 and/or are output to the external device
via the interface 18.

25 The detailed procedure for verifying that the image
data (I) and the digital signature corresponding to the
image data (I) were actually generated by the above
image input device is as follows.

30 (Digital Signature Verification)

The image data (I) and the digital signature
Dcam(SKman, Dcam(SKcam, H(I)) are verified by carrying
out an operation which uses the public key PKman, the
35 algorithm for verifying the digital data Eman of the
external device, the public key PKcam, the algorithm

for verifying the digital data Ecam, and the
compression algorithm H of the digital camera.

For example,
5           $H(I') = Ecam(PKcam, D'man(SKman, Dcam(SKcam, H(I'))))$.

If the equation holds, the image data (I') is the true
image daa that had been input by the digital camera.
10 On the other hand, if this equation does not hold, the
image data (I') will be understood not to be the true
image data (I). Accordingly, the verifier can determine
that the image data has been modified or forged.

15 (Another Embodiment)

This invention includes all image input devices and
systems obtained by combining each of the above
described embodiments.
20
Fig. 3 shows, in conceptual form, the construction of
the image input system with a verification function.
In Fig. 3, an image input device 30, similar to the
image input devices of the above embodiments, is
25 connected with a portable external device 31 via an
external interface 32. Also, a checking device 33 is
connected with another external device 34 to verify the
digital signature.

30 For example, the checking device may be a personal
computer which has an algorithm for verifying the
digital signature Ecam, the public key PKcam of the
image input device, the algorithm for verifying the
digital signature Eman, and the public key PKman of the
35 external device. Alternatively, the checking device
may be a personal computer connected to the external
device; and the external device may have an algorithm

for verifying the digital signature Ecam, the public
key PKcam of the image input device, the algorithm for
verifying the digital signature Eman, and the public
key PKman of the external device.

5

The term "image" in Fig. 3 refers to an object being
photographed ; and "(I)" refers to image data. An
image input device which is connected with the external
device 34 via the interface serves as the checking
10 device. The image data is fed selectively into the
generator (C-CODEC) 30a and into the external device 32
via the interface; and/or is output from the generator
30a to the interface 32.

15 As shown in Fig. 3, an adder or mixer 35 is provided
for adding or mixing the output from the generator 30a
or the external device 31 to or and the image data (I).

The output of the adder 35 is illustrated in Fig. 4.
20 The image data and the digital signature corresponding
to the image data (I) are packaged in a predetermined
unit as shown in Fig. 4.

It will be appreciated that if the image input system
25 uses the RSA cryptosystem, the input system output will
be only the digital signature. This is because the
image data can be recovered from the digital signature
in the RSA cryptosystem. Accordingly, even if the
input system does not have the CODEC system for data
30 compression, the system can record and/or communicate
only the digital signature without reducing the memory
capacity and the communication efficiency.

The system and the form of its output are shown in
35 Figs. 5 and 6, respectively. The image input device of
this invention need not be only a digital camera. It
may, for example, be a scanner, a copying machine, a

facsimile, a filing system, an optical character recognition (OCR) system, etc. Also, this invention is not limited to image data but it may be used for the processing of several other kinds of information.

5

According to the above described embodiments, the operator cannot generate the digital signature without the image input device or the external device which has the secret key and the algorithm for generating the

10 digital signature. Accordingly anyone can easily verify the correctness of the signature by using the public key and the algorithm for verifying the digital signature corresponding to the secret key and the algorithm for generating the digital signature,

15 respectively.

Thus, according to the above described embodiment, the image input device or the image input method can guarantee that the image data had been generated by the

20 image input device or system without modification or forgery; and it can guarantee the authenticity of the digital information as well as the image data, the audio data, etc., as evidence Thus, this embodiment can be used to protect from the malicious use of

25 digital information.